加餐 | 数据安全：如何防止内部员工泄漏商业机密？

2020-01-10 何为舟

讲述：何为舟
时长 08:50　大小 7.08M

你好，我是何为舟。前面讲了这么多期正文，今天，我们通过加餐，来聊一个比较轻松的话题，数据安全。

我们先来看一个新闻。2017 年，公安破获了一起涉及 50 亿条个人信息泄漏的重大案件。经调查发现，犯罪嫌疑人竟然是京东的一名试用期员工郑某鹏。还有非官方的消息说，这个郑某鹏，先后在亚马逊、新浪微博等知名互联网公司，利用试用期的员工身份，下载用户的隐私信息进行倒卖。

如果你稍微关注过这方面的新闻，就会发现，这种事情真的不少。Code42 在 2019 年发布的数据泄漏报告称，有 69% 的公司承认员工曾泄漏过公司数据。其实，这些数据泄漏的行为就是我们要关注的数据安全。

从广义上来说，数据安全其实是围绕着数据的 CIA 三元组来展开的。我们之前讲过，应用的本质就是数据，因此，我认为任何与安全相关的内容，其实都可以涵盖到数据安全中去。那从狭义上来说，数据安全就是如何防止员工泄漏公司的敏感数据。国内公司主要关注的还是狭义上的数据安全，因此，我们今天所要讨论的也是狭义上的数据安全。

为什么员工会主动泄漏公司机密？

那作为员工，为什么会主动泄漏公司数据呢？我曾听过这样一句话，觉得非常有道理：“生活中有两个悲剧。一个是你的欲望得不到满足，另一个则是你的欲望得到了满足。”人的欲望总是无穷无尽的，而且一旦萌生，就极难克制。对于大多数人来说，泄漏公司机密，无非有以下几个常见的出发点。

我认为，第一个肯定是赚钱，这也是最容易想到的一个。员工利用公司来赚钱的方式，无非有 3 种。

倒卖公司数据。对于任何一家公司而言，数据一定是其最有价值的部分。而员工往往能够很轻易地获取到一些私密的内部数据。在黑市上，个人的姓名、手机号和住址等信息，都能够以每条几毛甚至是几块的价格进行交易。除此之外，竞争对手之间，也很乐意出高价来收购对方的商业机密。

欺诈。最典型的就是“吃回扣”，也就是利用公司采购流程的漏洞来获得非法收益。比如，一个和电商有关的欺诈行为，就是员工给自己发放内部网站的高额优惠券。

贪污。采购投标、拉拢客户这些环节，都极容易出现贪污现象。

第二个出发点，我认为可能是员工出于对公司的不满而实施的报复行为。互联网公司往往变化非常快，员工被公司突然裁掉的事情这几年屡见不鲜。被裁员工心怀不满也是常事。除此之外，一些主动辞职的员工，出于对现阶段工作内容和收入的不满意，也会心生怨怼。我们常常拿来当玩笑说的“删库跑路”就是最常见的报复行为。

第三个出发点就是跳槽。说白了，就是跳槽后的员工，以原公司的核心数据为资本，服务下一家公司。我们经常能够听到相关的新闻报道，比如，某个销售总管跳槽，把客户也一并带走了；或者某个 leader 带着得力员工一起跳槽。这些客户关系或者员工，其实都是公司的核心资产。所以，一个内部员工，可以将他手中的这些资产，作为跳槽的一个筹码，来实现个人的职业发展。

第四个是商业间谍。这个你应该在很多商战类的电影和电视剧中经常看到，这些间谍会为了原始公司的利益打入对手公司的内部。这样的员工一开始就是怀揣着某种目的进入公司的。除此之外，一些黑灰产的从业人员也可能为了窃取某个公司的数据，去应聘这个公司。

第五个其实和利益就没有直接关系了，只是员工为了满足自己想要炫耀的心理，对外泄漏信息。尤其是某些大公司的员工，他可能为了证明自己能够知道一些内部消息，而将内部的活动规则、公司通告等在微博或者脉脉上进行宣扬。这些敏感信息的泄漏，对于公司的正常运营以及声誉，都有可能产生非常严重的影响。这也就是所谓的“员工一张嘴，公关跑断腿”。

如何防止内部员工泄漏机密？

现在，我们大概知道了，员工一般会出于什么心理去泄漏机密。了解了这些问题的“源头”，我们就需要思考，如何基于这些情况，做好数据安全，防止出现泄密情况。

我认为，在数据安全上，我们能做到的防护其实十分有限。因为数据安全所面临的威胁，不仅复杂度很高，而且隐蔽性极强。所以，我们只能通过各种手段，尽可能地降低数据安全带来的影响。下面，我总结了几个可行的方法和手段。

最直接的方式就是背调。背调是公司用来评判人品的一个直接方式。公司通过对员工过往工作行为和资历的调查，就能够看出员工是否值得信任。但我们不得不承认，一个公司在背调时，能够获取到的信息十分有限，根本没有办法和公安、政府相比。这也导致背调的准确性得不到保证，比如开头提到的郑某鹏，他能够以应聘者的身份入职多家知名公司，就是因为这些公司在背调时没有发现他的真正目的。

那除了前期招聘时的背调，我们还有什么其他方法来做防护吗？当然是有的。

DLP（Data leakage prevention，数据泄漏防护系统）应该是目前数据安全中，最基础也是最重要的技术防护手段之一了。从原理上来说，DLP 就是监控公司内部所有的数据流动，对数据的内容、类型和流向等进行统计和分析。不过，目前的 DLP 产品，更多的是关注员工个人设备中的数据流动。这主要是因为相比于服务器，个人设备的使用范围更广，不容易控制。而且，服务器的数据流动太大，监控成本也过高。

那 DLP 是如何监控数据流动的呢？一般情况下，公司在部署了 DLP 产品之后，会强制员工在电脑上安装一个 DLP 的终端。公司会通过这个终端，监控员工设备中的各种数据流动。

换一句话说，只要公司需要，可以随时掌握员工在个人电脑上获取了哪些数据、进行了哪些操作。不得不说，这确实在一定程度上侵犯了员工的个人隐私，但这也是目前公司为了保障数据安全，所采取的一些不得已的手段。

另外，公司还可以对员工的行为进行异常检测。为啥要这么做呢？这是因为，一个员工，如果想要贩卖公司的数据，那他就需要获取自己职责之外的大量数据。比如，如果一个客服在下班之后，还频繁地查询用户的个人信息，那么这个客服就很有可能在窃取公司的隐私数据。想要对员工的行为进行异常检测，公司需要先对各类员工的行为进行采集和数据分析，然后制定对应的规则和模型，从而区分员工的正常行为和异常行为。

最后，公司还可以制定相应的规章制度，对破坏公司利益的员工进行处罚和公示，这些都能够对员工产生威慑作用，从意识和心理上阻止员工泄密。

总结

好了，今天的加餐内容就是这些。虽然说，关于数据安全的防护，我们主要是站在企业的角度来讨论的。但是这些违法事件的发生，还是给我们自己“敲响了一个警钟”。提醒我们要坚守自己的道德底线，不去做违法的事情。

思考题

最后，还是给你留一道思考题。你见过哪些泄密行为？这些行为对被泄密的公司产生了什么影响？如果可以的话，你可以讲讲，你们公司是如何防止员工泄密的。

欢迎留言和我分享你的思考和疑惑，也欢迎你把文章分享给你的朋友。我们下一讲再见！

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇　14 | 网络安全：和别人共用Wi-Fi时，你的信息会被窃取吗?

精选留言 (6)

写留言

qinsi
2020-01-10

阿里巴巴公司根据截图查到泄露信息的具体员工的技术是什么？ https://daily.zhihu.com/story/8812028

> 作者回复: 可以了解一下图片水印的技术，可以将内部邮件、wiki、钉钉等软件内的图片甚至页面本身，加上水印，水印跟当前登录的用户作关联，就可以查出来了。不过据我了解的，目前图片的水印技术，除非是明显的加在图片背景中，否则各类隐藏式的水印，基本拍张照片，就都没了。

1

柒月
2020-01-10

我同事从一家公司离职，把他电脑都拆了，硬盘也卸掉了。

leslie
2020-01-10

看企业大小：不同级别的企业有不同级别的处理方式，同样因此可能就带来一些不便或涉及隐私问题。早期最简单的方式就是电脑封端口、监控网络流量、工作电脑后面有监控、以及核心操作全部在堡垒机东西某些传输权限掌握在部门管理层。

展开

小晏子
2020-01-10

没见过，听说过某司员工从公司的实验室里的服务器上盗取源代码，但他不知道这个实验室里有摄像头，就被完整的拍下来了，最后就被送进去了...

展开

Cy23
2020-01-10

大公司还好点，职责分开，小公司就不好办了，来个新员工，没多久就把公司所有代码都拷贝走了

作者回复: 其实职责分离也挺难做到的，比如应用有个逻辑需要用户的手机号，那是不是开发就能够看到所有用户的手机号呢?

陈优雅
2020-01-10

具体实施呢？装监控终端？

展开

作者回复: 安装DLP，然后进行数据分析，这是比较普遍的手段